



Zoom Meeting Interface and Basic Logistics



*image above is a publicly available tutorial image obtained from Zoom website

- **VIDEO:**
 - **Panelists/Presenters/Facilitators** - Please enable your video using **bottom left video button with camera icon.**
 - **Attendees** - If you did not receive an invitation to be a panelist, you are in attendee only mode and **will not have access to enable video**
- **AUDIO:**
 - **Panelists/Presenters/Facilitators** - Adjust your audio settings as needed (choose computer audio, call in, mute, etc.) using **audio button bottom left, microphone icon. Please remain muted unless speaking.**
 - **Attendees** - If you did not receive an invitation to be a panelist, you are in attendee only mode and **will not be able to enable audio**
- **CHAT:** The chat function is open to **ALL** participants (bottom, middle right, highlighted in orange in this image). Those in Attendee only mode are encouraged to provide feedback and questions via chat throughout the discussion. Chat will be monitored by the *FAST* team and key themes will be pulled into the discussion.
- **TECHNICAL DIFFICULTIES:** Having trouble hearing the presenters or seeing the shared screen? Put your issue in chat and the Meeting Host will help you.



The Role of Trust Framework(s)

ONC *FAST* Workshop
September 14, 2020



FAST Taskforce Antitrust Notice

- The ONC FHIR At Scale Taskforce (*FAST*) (Hereinafter “Taskforce”) is committed to full compliance with existing federal and state antitrust laws.
- All members involved in the Taskforce effort, including its advisory groups, will comply with all applicable antitrust laws during the course of their activities. During Taskforce meetings and other associated activities, including all informal or social discussions, each member shall refrain from discussing or exchanging competitively sensitive information with any other member. Such information includes, but may not be limited to:
 - Price, premiums, or reimbursement charged or paid for products or services
 - Allocation of customers, enrollees, sales territories, sales of any products or contracts with providers
 - Any other competitively sensitive information that is proprietary to a member company
- If you have any specific questions or concerns, seek guidance from your own legal counsel.
- Members should not bring confidential information or intellectual property (hereinafter “Intellectual Property”) owned by their respective member companies into Taskforce meetings. To the extent such Intellectual Property is shared with the Taskforce that shall not be construed as a waiver of member company’s rights to, or ownership in, the Intellectual Property.



Session Facilitator



PAUL OATES

*Senior Enterprise Architect and
Lead for the IT M&A Practice*

Cigna

FAST Chief Architect





Agenda

- **Welcome & Introductions**
- **Session Goals**
- **Overview**
- **Discussion Topics**
 - Interactive Panel
 - Participant Q&A
- **Wrap Up/ Key Takeaways**





FAST Panelists

FAST Panelists	
<i>Luis Maas</i>	<i>EMR Direct, FAST Security Tiger Team Lead</i>
<i>Julie Maas</i>	<i>EMR Direct, FAST Identity Tiger Team Member</i>
<i>Alex Kontur</i>	<i>HHS ONC, FAST Directory, Versions & Scale Tiger Team Member</i>
<i>Bryan Scott</i>	<i>Humana, FAST Exchange Tiger Team Member</i>





Roles & Logistics: Panelist vs. Attendee Modes

FAST Key Panelists

- Invited to join, actively engage and support the conversation
- Encouraged to communicate verbally (mics on) and to turn on video
- Monitor the attendee chat box for feedback, address questions via chat or promote questions that are significant to the discussion topic or warrant a verbal debate /reaction with the panel group

Industry Expert Reaction Panelist (in panelist mode)

- Invited to join the live interactive discussion with the *FAST* team
- Encouraged to communicate verbally (mics on) and to turn on video
- Provide their industry expertise and feedback
- Discuss or debate the topic with the facilitator and the panelist group
- Raise questions or concerns
- Feedback will inform *FAST* next steps

General Audience and *FAST* Technical Learning Community Members (in attendee mode)

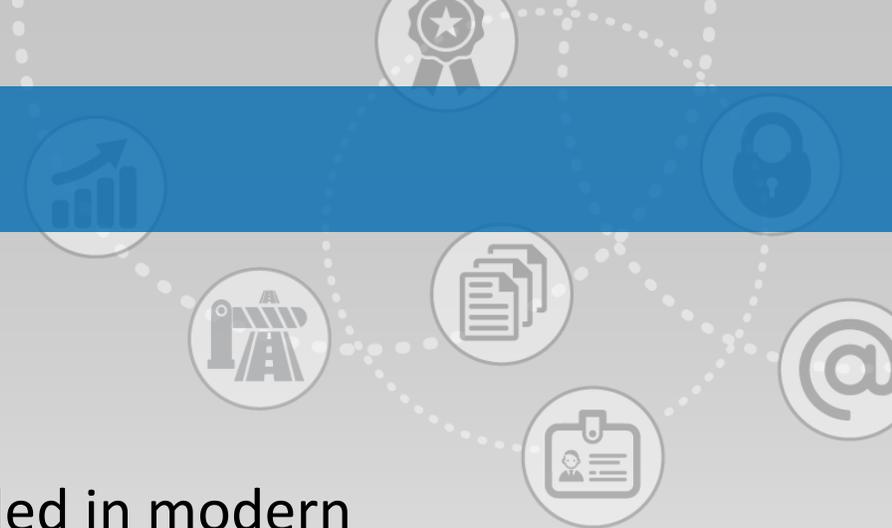
- Encouraged to engage and contribute feedback and questions via the chat box
- Do not have the ability to contribute verbally to the conversation (mics off)
- No ability to be on video



The Role of Trust Framework(s)

Session Description

FHIR is known for its capability to support integration needed in modern healthcare to achieve integrated care delivery. A key component of running FHIR at scale is predicated on the ability for transactions to cross trust frameworks. An open discussion on how the technical approaches determined by or impacted by trust frameworks fit into this model would be fruitful.





The Role of Trust Framework(s)

Session Goals

1. Consider how “trust frameworks” fit in the model of evolving FHIR-enabled interoperability.
2. Given the multitude of technical approaches determined or impacted by trust frameworks (HIE-based, or Direct), consider if there are particular challenges and opportunities for trust frameworks in achieving FHIR-enabled interoperability at scale.

Approach

1. Quick review of *FAST* solutions & why trust frameworks
2. Discuss the need: value and role
3. Discuss characteristics we need and gaps → most of our time here
4. Discuss how to mobilize and what is needed from *FAST* on this topic

Overview

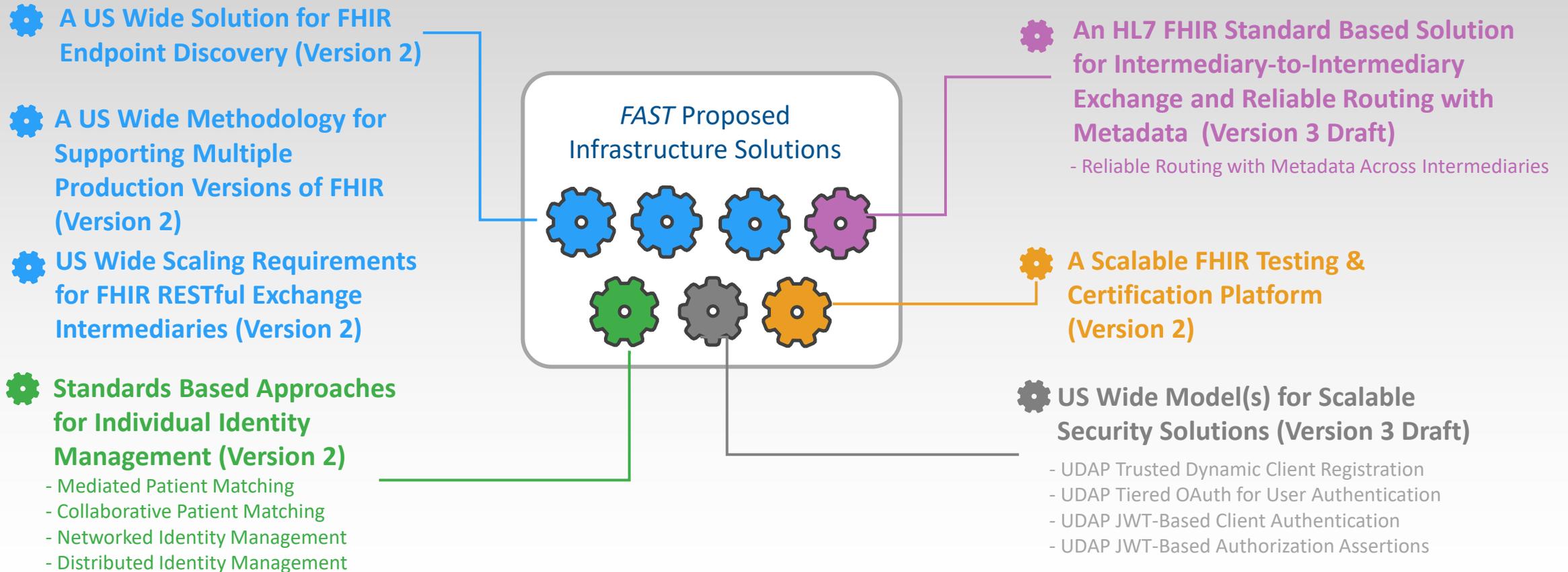
Short Review of *FAST* Solutions and “Why Trust Frameworks”





FAST Proposed Solutions

■ Directory, Version & Scale (3) ■ Identity (4) ■ Exchange Process (1) ■ Testing & Certification (1) ■ Security (4)



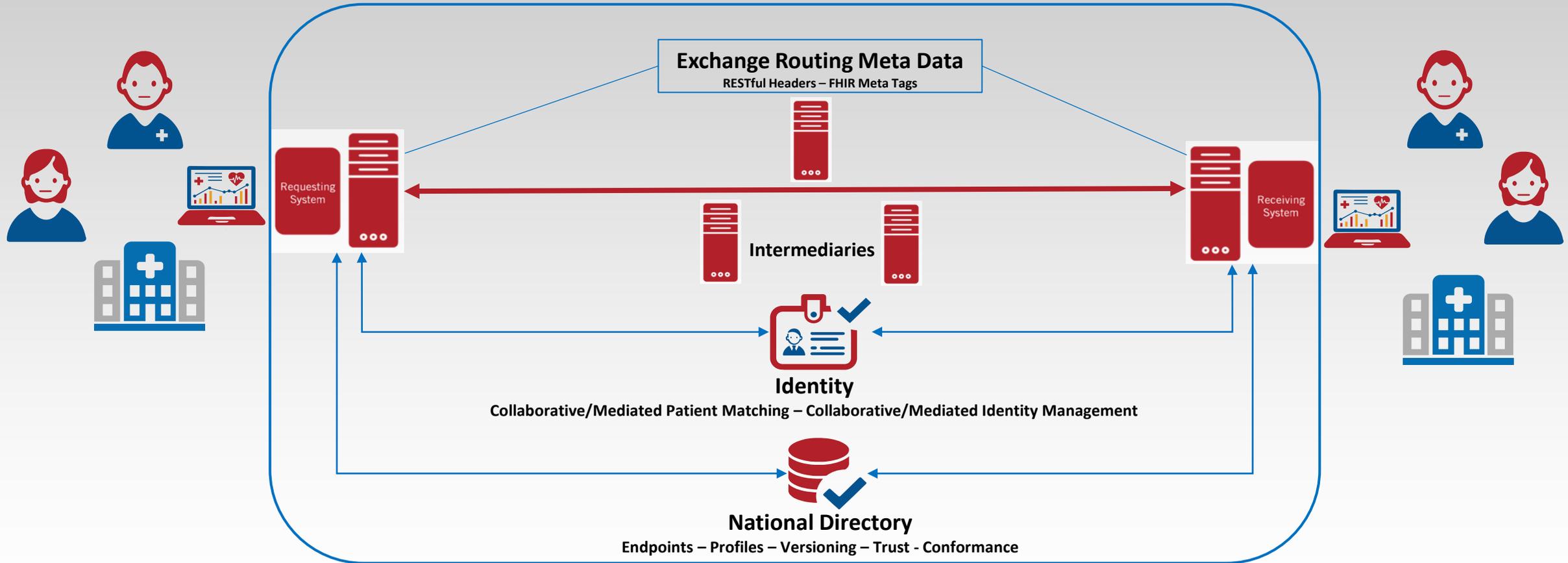


Conceptual Integrated Architecture



Security (Authenticate/Authorize)

UDAP Trusted Dynamic Client Registration - UDAP Tiered OAuth User Authentication - UDAP JWT-Based Client Authentication - UDAP JWT-Based Authorization Assertions



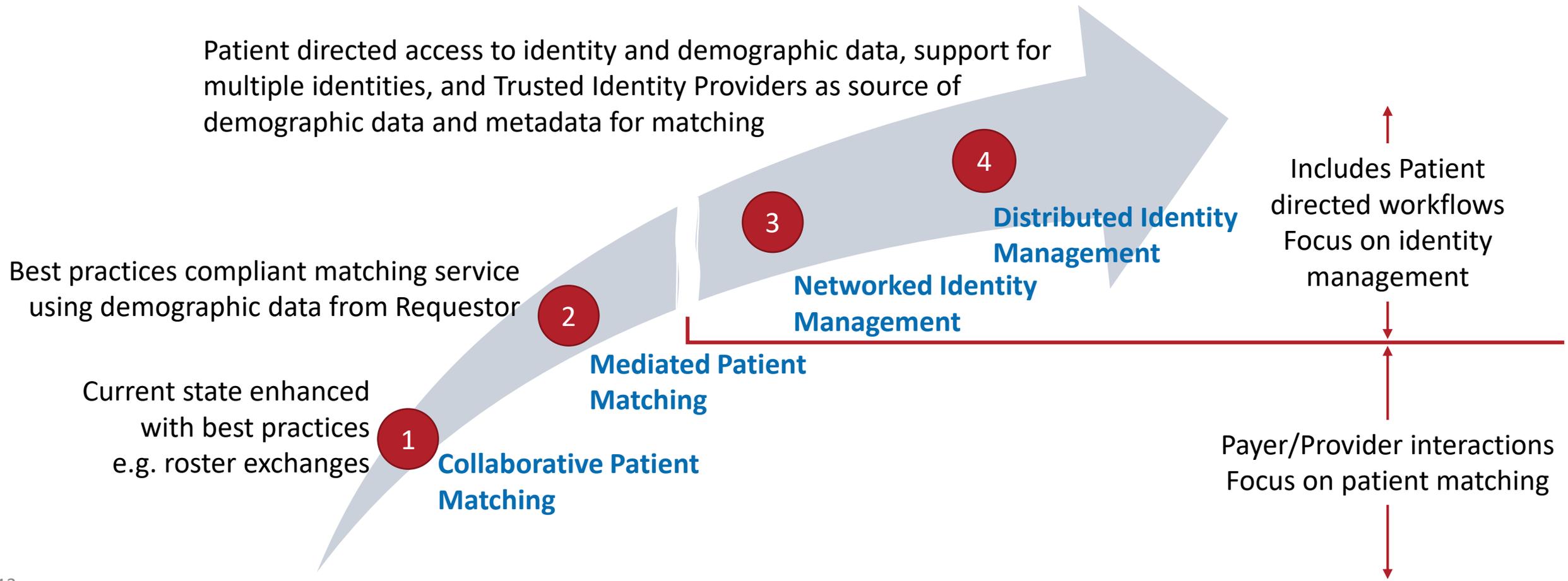
CONFORMANCE & CERTIFICATION (Testing & Certification Program)

PILOTS (FAST Capability Vetting with Existing HL7 Accelerators)



FAST Identity Management Solution Options: Low to High Complexity

Multiple options progressing from low to high complexity (technical and process)

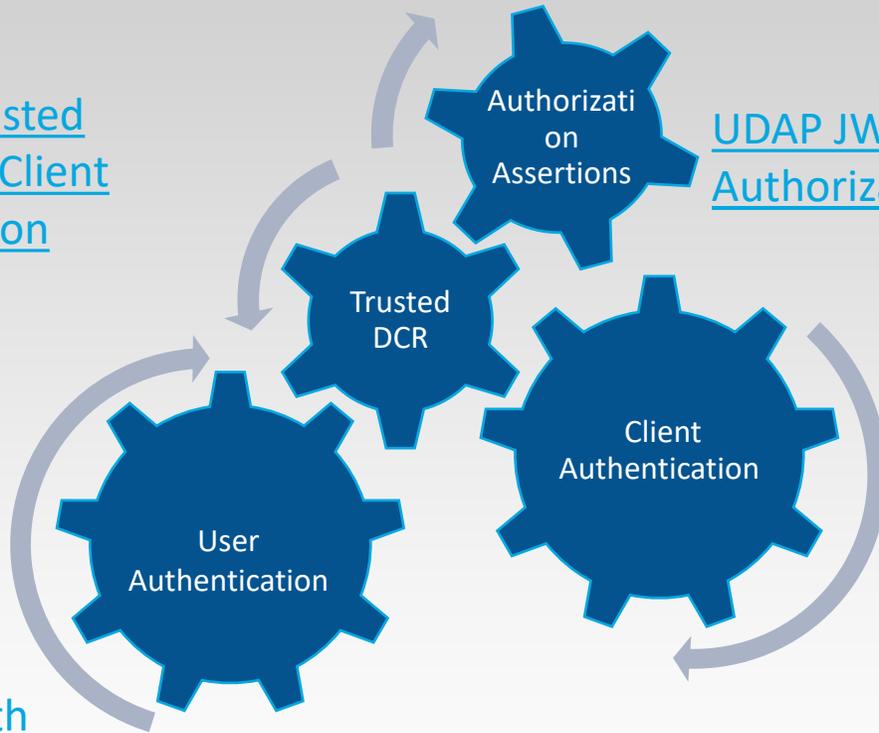




FAST Security Proposed Solution: Trusted Ecosystem

UDAP Trusted Dynamic Client Registration

UDAP JWT-Based Authorization Assertions



UDAP JWT-Based Client Authentication

Reusing established digital identities (i.e., leverage existing PKI infrastructure)

- Many organizations have established digital identities that can be reused within a trust community for FHIR transactions.
- Digital identities, expressed in digital X509 certificates, enables the requestor to authenticate itself to a responder's endpoint.
- The use of these digital identities helps to remove the burden of credentials management among FHIR transaction participants – paving the way for scalability within the FHIR ecosystem

UDAP Tiered OAuth

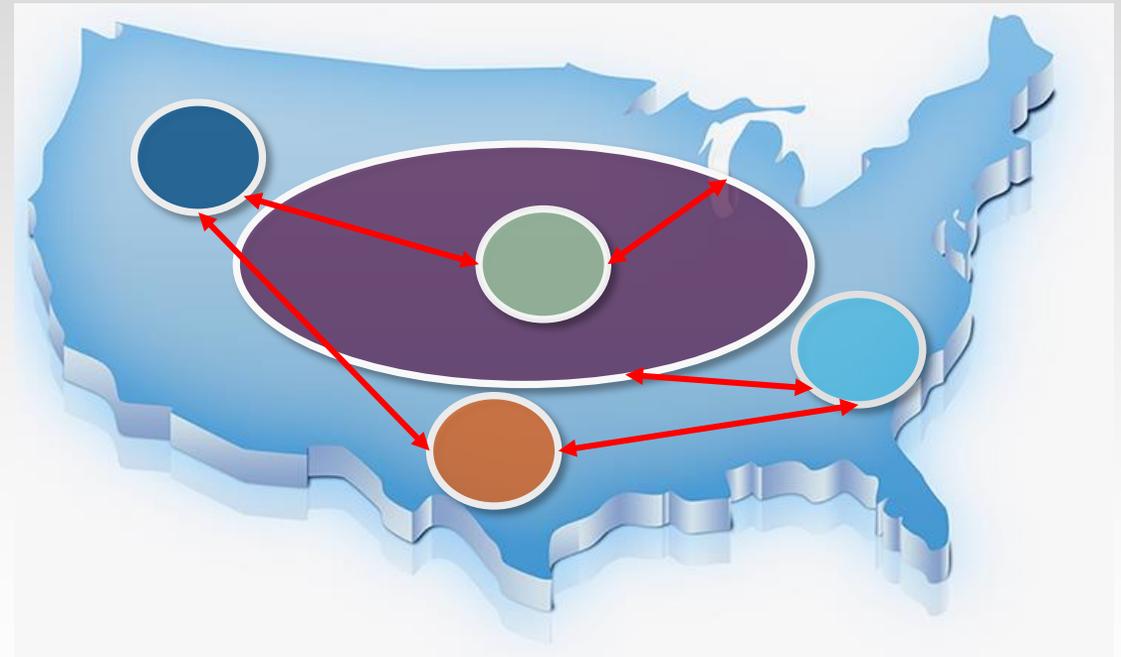


What Do We Mean by Trust Frameworks?

Language: Trust Framework, Trust Networks

Working definition for this session:

- A community of trust with respect to security and identity that agrees to:
 - Policies
 - Operating rules
 - Technical approach





Base Characteristics of a Trust Network

- Policies (behaviors, legal protections)
- Operating Rules (purpose of inquiry, refusing a connection responses, can't find patient responses, hierarchy of local consents)
- Technical Approach (certificate formats, match data structures)





Some Examples

Of Networks:

- Visa Card Network
- Safe Bio Pharma
- Direct Trust
- Commonwell
- CareQuality
- etc

Of Enablers and Forums:

- UDAP (in the *FAST* solutions)
- NIST, ISO standards
- Kantara
- IdentityNext
- ICAM
- etc

There are many activities in healthcare and out of healthcare that are working on how to reduce interoperability friction through trust standards and network implementations

Discussion #1 – Value, Need and Role of Trust Networks in FHIR Scale





Discussion: The Need for Trust Frameworks to Scale FHIR Adoption

?

As *FAST* and FHIR scale matures, where do we see trust models fitting in?

Option 1

Trust frameworks are useful, but not really required. We can implement sufficiently across our partner stakeholders with out them

Option 2

The path to scale FHIR efficiently is through some common approach via Trust Frameworks

Discussion #2 – Characteristics of Trust Networks

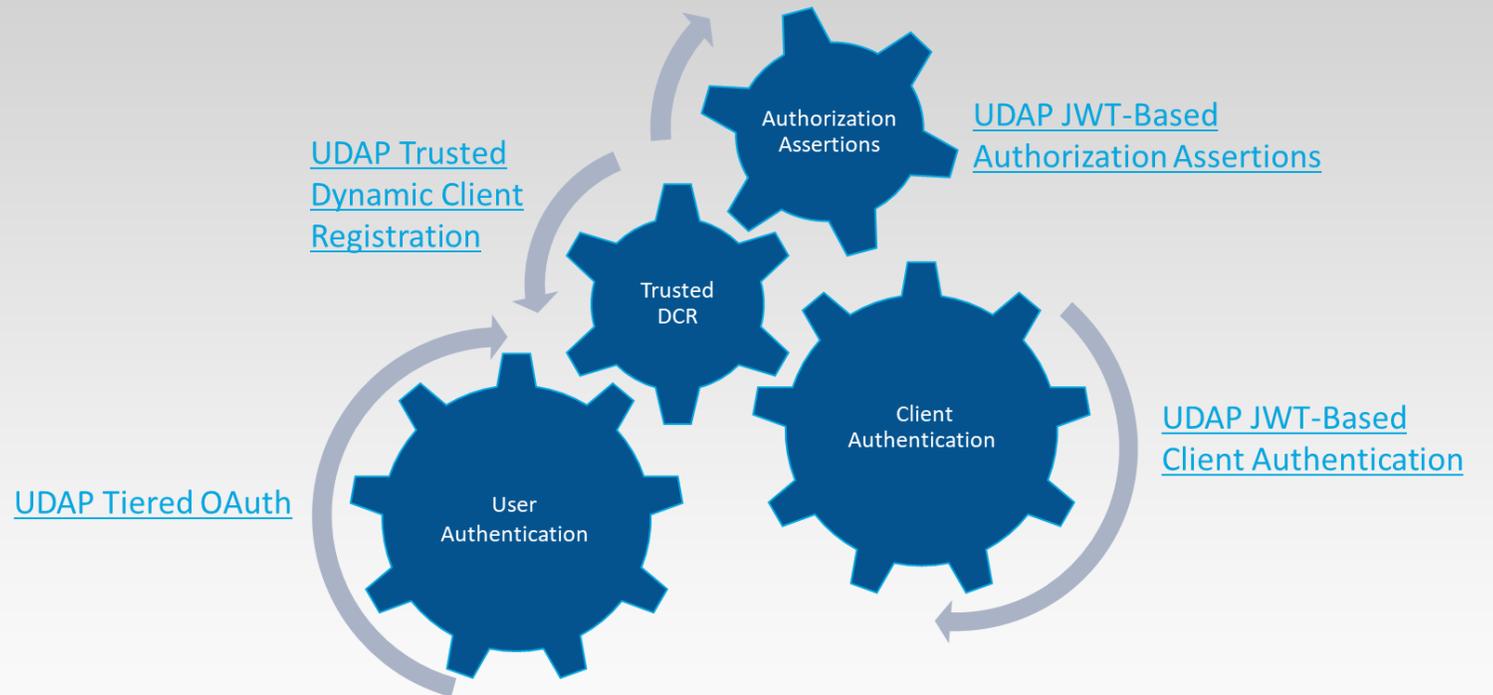




Discussion: How Trust Networks Enable Security Solution

?

How are dynamic client registration, tiered OAuth etc. enabled in a trust framework?



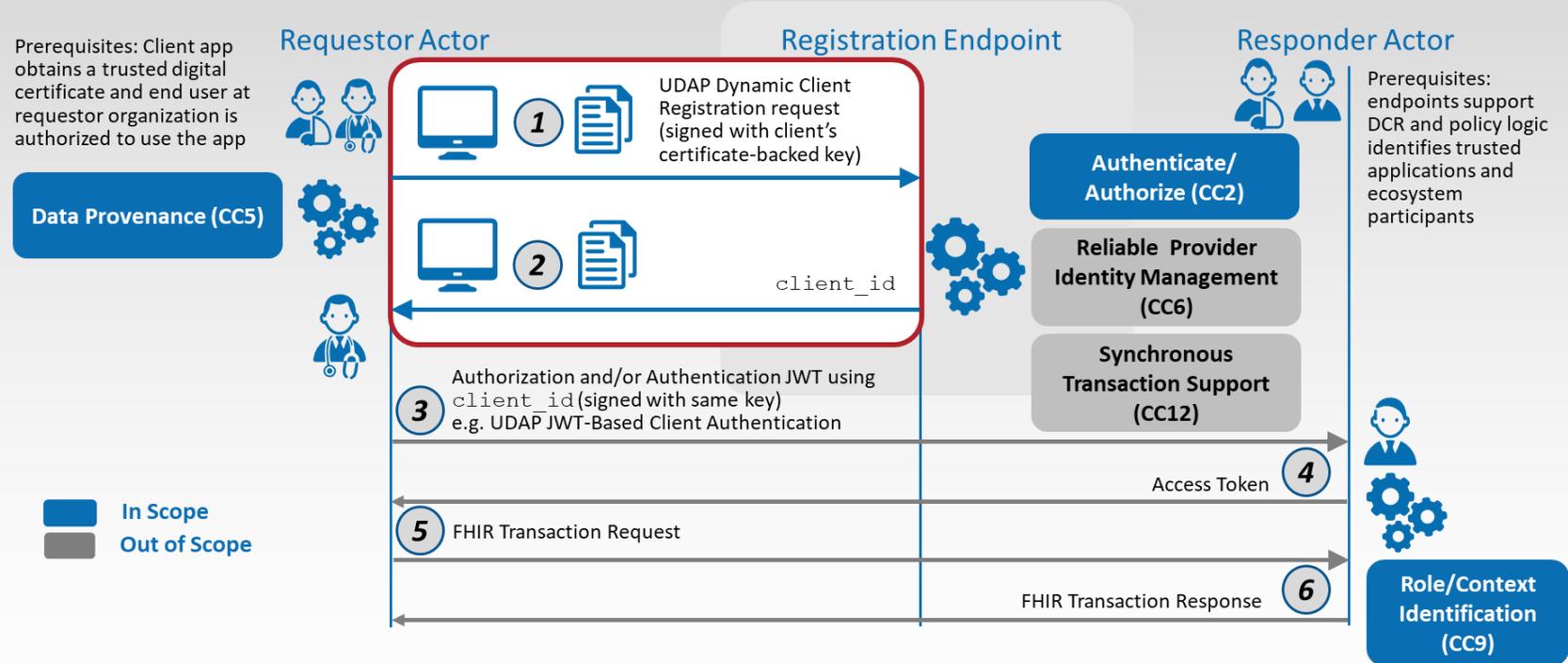


Discussion: Dynamic Client Registration



What are the benefits of Dynamic Client Registration (DCR) and what is still needed to maximize scale?

Who would/could build the missing layers to work with DCR and advance scale?



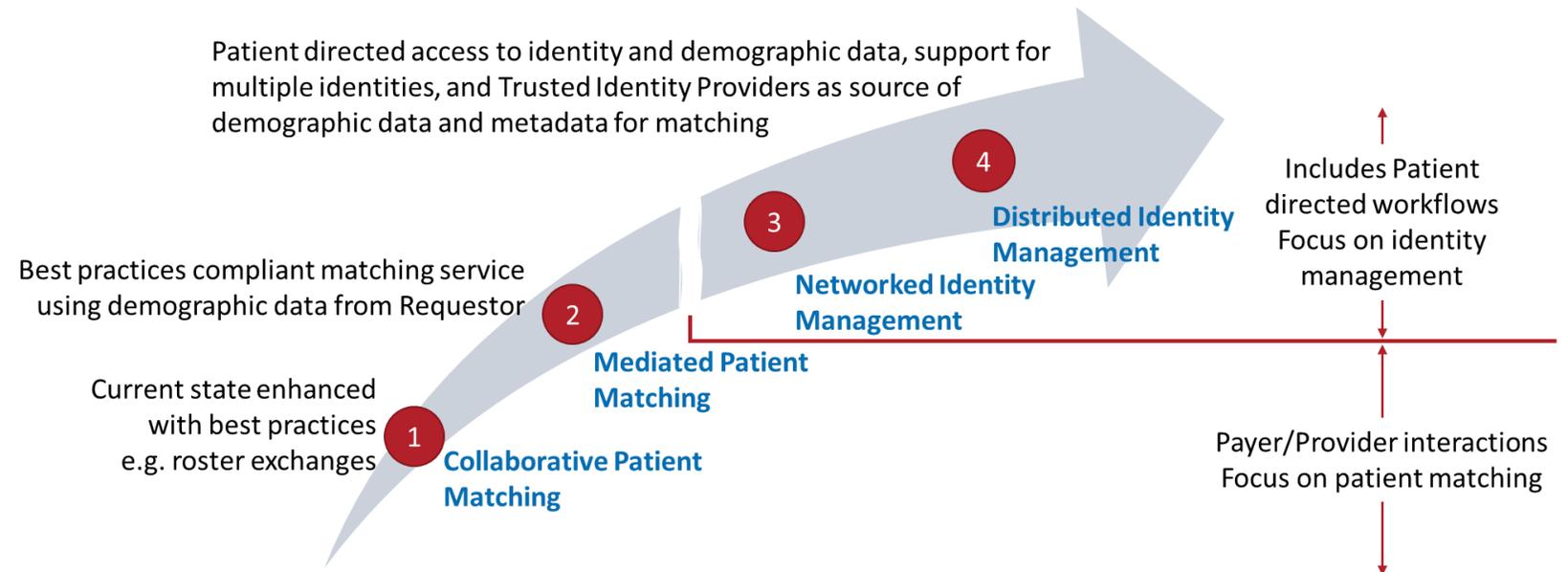


Discussion: How Trust Networks Enable Identity Solution

?

How could patient matching solutions be enabled more efficiently if done within a trust framework?

Multiple options progressing from low to high complexity (technical and process)





Networked Identity Management



 In Scope
 Out of Scope

Key Features

- Patient-directed
- Builds on capabilities required by Cures Act
- Use of Digital Certificates
- Authentication is in scope
- Allows for out of band communication/resolution
- No exchange of rosters required
- Metadata from OpenID credential used for local matching



1

Prerequisite: **Subject uses a credential such as a patient portal account** (or other trusted OpenID Connect Issuer) with ability to allow Responder to obtain verified demographic info from profile

Data Provenance (CC5)

Role/Context Identification (CC9)

Requestor Actor

Responder Actor

Networked Identity Management via **Subject's Own OpenID Credential and Authorization Code Flow via Tiered OAuth**

Uses metadata to match locally.

If Subject of Requestor's query cannot be resolved, Responder may contact Subject or Issuer for additional information e.g. out of band resolution



Authenticate/ Authorize (CC2 a & b)

Reliable Provider Identity Management (CC6)

Reliable Patient Identity Management (CC4)

Synchronous Transaction Support (CC12)



2



FHIR Request with profile information about **Subject**

3 CSP



4



FHIR Response

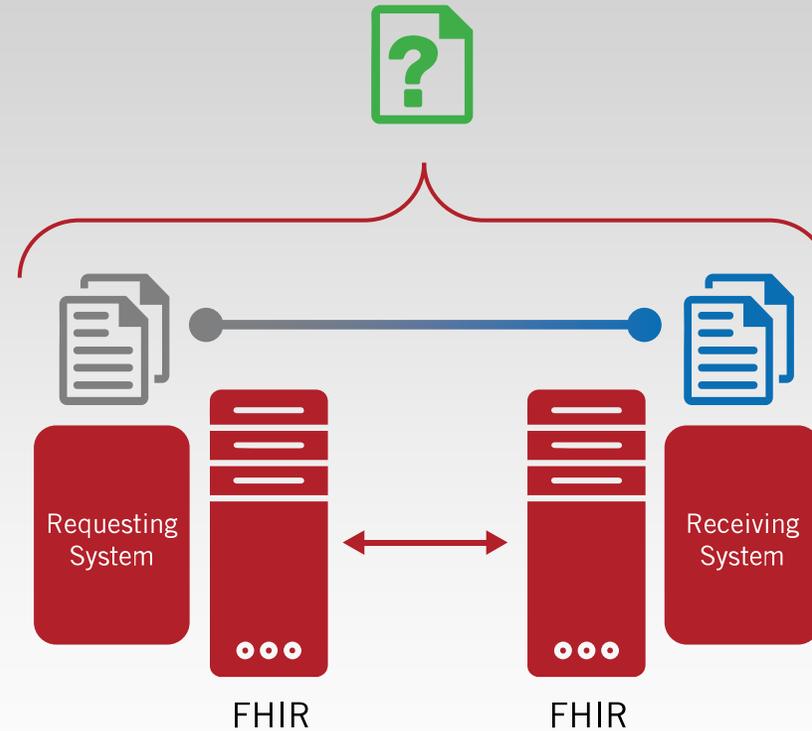




Discussion: Mixed Stakeholders/Purposes

?

If Hospital A is part of a trust and wants to exchange data with Payer B in a different trust, how do *FAST* capabilities play in that scenario (e.g. to do the UDAP or agree on a patient match)?





Discussion: Scaling Trust Networks

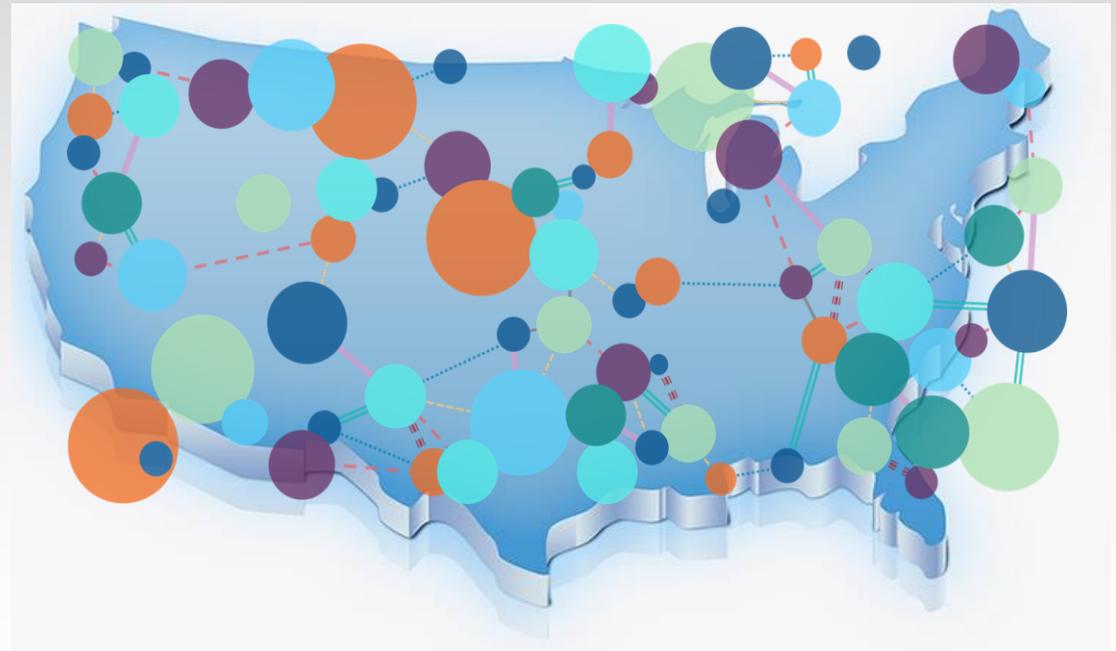
Given likelihood of trust frameworks, is there agreement that we need interoperability between trust frameworks to blanket the country?

?

How do trust networks scale?

Are there practical limits?

How can we keep extending the network based on the established trust in today's environment and where/how would *FAST* support this?





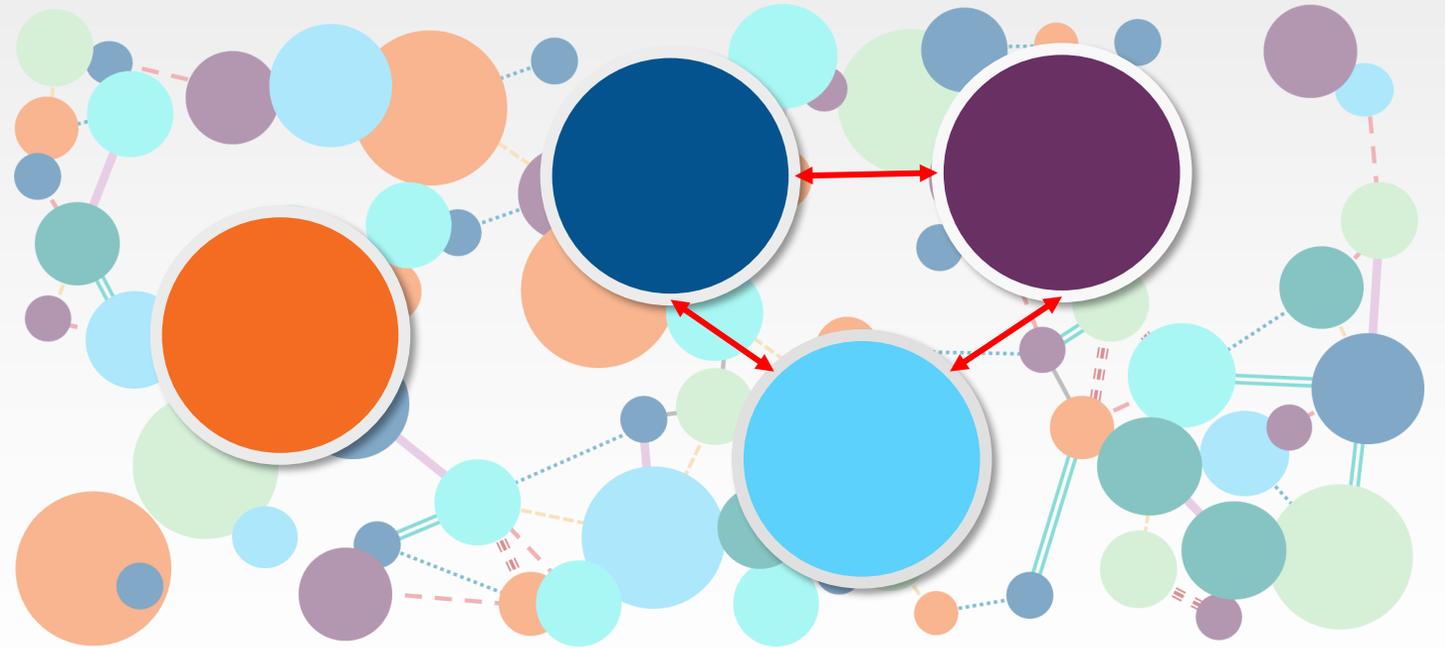
Discussion: Trust Network Allowable Exceptions for Members

?

If you belong, do you have to exchange with everyone the network trusts?

Do all trust networks have to trust each other?

What are reasonable exceptions?

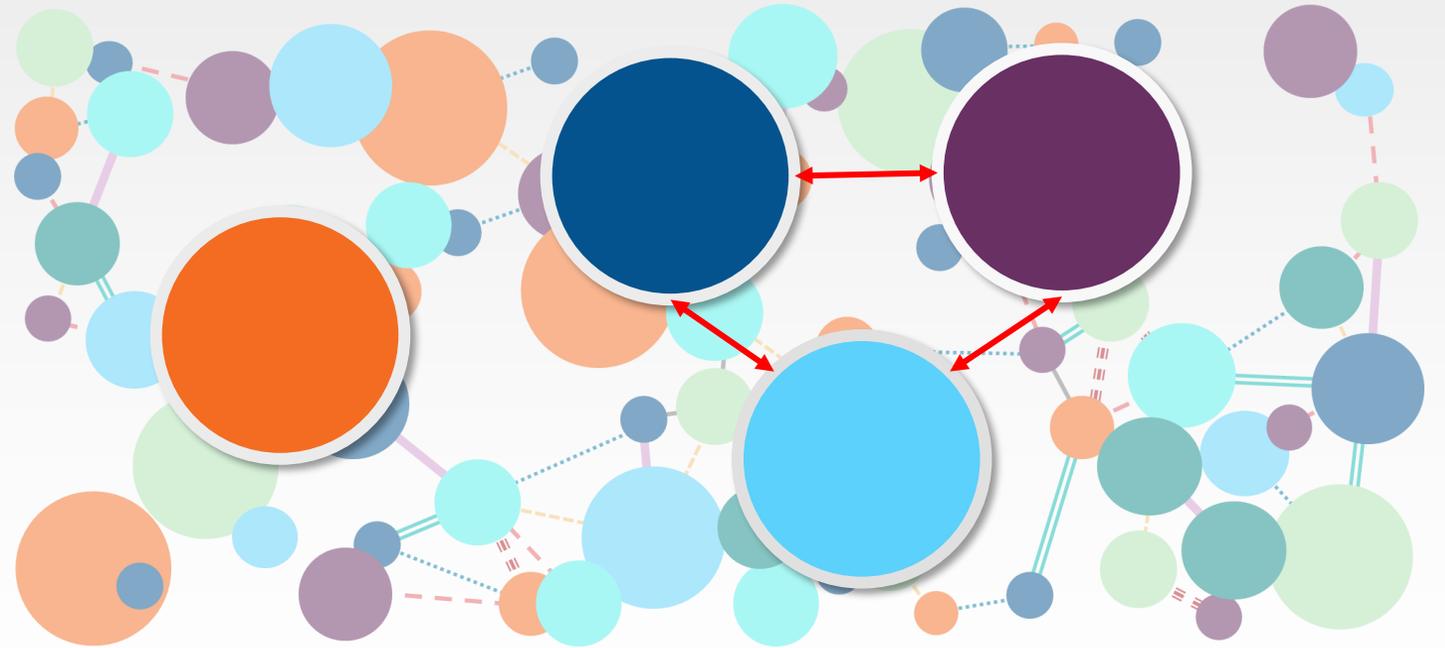




Discussion: Knowing One's Trust Network

?

In the directory, when you look up an endpoint, what meta data is needed to say “I belong to these networks”

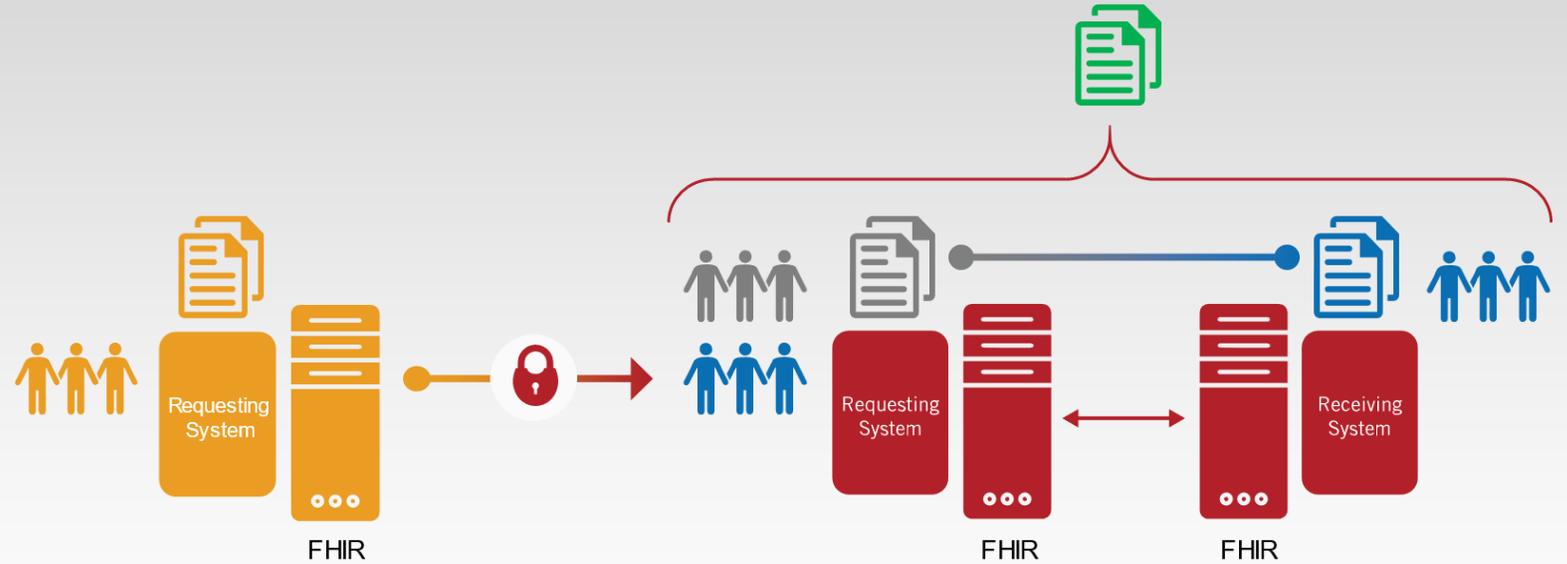




Discussion: Watching for Barriers, Overhead

?

How do we position the *FAST* work to allow trust framework communication, but doesn't result in creating barriers to implementation?



Discussion #3 – Mobilizing Trust Frameworks





Discussion: Some Known Deployment Items



What are some of the early items identified that *FAST* needs to support?

Early Enablers List

- Guidance on how to deploy - number of trust networks, how keep number of certificates to a manageable level
- IG language that enables reasonable discovery work, use of directory vs. capability statement approaches for knowing who you belong to
- Set of aligned policies and technical IG so trust networks have a common baseline
- Rules of the road when something goes wrong. Potentially a "must clause" at the national level so local variations have boundaries that don't inconsistently disrupt. So need not just the tech IG, but the reciprocity and rules too
- A set of purpose of use explanations that are widely known and handles special purposes
- Continue/advocate for the model on how consent is carried across jurisdictions
- Determine the level of IG - one generically and one for each purpose of use? and define the granularity that will actually work in implementation (payment, treatment) and have as the common policy/network template that enables cross-network trust
- Ensure that there is always a response that enables requestor to know where they stand why the responder responded the way they did, including the simple "I just don't know who you are or don't agree you have that purpose"

Find the community where this is going to be navigated – next slide...



Discussion: Who Mobilizes the Trust Frameworks

What options do we have to further define and mobilize trust frameworks?



Who/Where/How do we establish policies, operating rules and agree on the technical approaches for *FAST*-enabled Trust Networks?

Should these be consensus, standard and/or regulation?



Wrap Up





Breakout Sessions Schedule

12pm – 1pm: Lunch Break

1:00pm – 2:30pm: Afternoon Breakouts Part 1 - *FAST* Pathways to Implementation (limited attendance, concurrent)

Room #1:
Standards

Session Goals:

1. Determine which requirements can be part of existing standards vs. the need to create new standards.

Room #2:
Regulations

Session Goals:

1. Consider the current regulatory landscape and how it presents opportunities or challenges related to each of the proposed solutions.
2. Explore policy concepts and considerations that would allow for transparent and predictable update cycles in response to industry need.
3. Discuss ways to mitigate impact of understanding and implementing regulatory requirements for smaller organizations.

Room #3:
Process

Session Goals:

1. Explore process related elements for implementation of FHIR-enabled interoperability at scale (e.g., process related governance, funding, and operational considerations, etc.)
2. Identify key things necessary to deploy solutions in a sustainable manner.
3. Explore limitations and opportunities to convene related groups that need to avoid any implication of anti-trust.



FAST Workshop – Full Day Agenda and Resources

- View the [FAST Workshop Summary and Detailed Agenda](#)
 - Morning and Closing Plenary
 - Breakout Room Sessions Schedule
 - Handouts and Resources
- Explore these *FAST* resources
 - New to *FAST*? Breakout sessions target interactive discussion and references the *FAST* work to date. Please consider exploring any of the following *FAST* artifacts before attending these breakout sessions:
 - [The FAST 2020 Mid-Year Report](#)
 - [The FAST 2019 End of Year Report](#)
 - [SME Panel Session Pages](#)

CONTINUE THE CONVERSATION!

Join the Technical Learning Community to stay up to date – receive updates about FAST presentations & events, provide additional input and follow our progress.

[JOIN THE LINKEDIN GROUP](#)

&

[SIGN UP FOR THE TLC](#)

All content is available on the [FAST Project Page](#) or <https://tinyurl.com/ONC-FAST>



Thank You

Connect with *FAST* on [LinkedIn](#) to stay informed

For more information on the *FAST* Initiative,
visit the *FAST* [Project Page](#) or <https://tinyurl.com/ONC-FAST>

Have any further questions/suggestions?

Please contact Stephen Konya at Stephen.Konya@hhs.gov
& Diana Ciricean at Diana.Ciricean@hhs.gov